

Remarks:

Reconsideration of the above referenced application in view of the enclosed remarks is requested. Applicant thanks the Examiner for withdrawing the previous rejections. Claims 1, 3-11, 13-17, and 19-32 remain in the application.

ARGUMENT

§ 103 Rejections

Claims 1, 3, 5, 6, 8, 10, 13, 16, 17, 19, 21, 22, 24-30 and 32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over USPN 6,009,524 to Olarig et al. (hereinafter, "Olarig et al.") in view of USPN 6,374,357 to Mohammed et al. (hereinafter, "Mohammed et al."). This rejection is respectfully traversed and Claims 1, 3, 5, 6, 8, 10, 13, 16, 17, 19, 21, 22, 24-30 and 32 and their progeny are believed allowable based on the following discussion.

The Examiner asserts that Olarig et al. teach *receiving, at a BIOS in a system, a message from an authorized party, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor*. However, at the cited reference (Col. 4, lines 1-15) Olarig et al. teach that a system administrator receives a BIOS update and examines the update for verification. The administrator adds an additional digital signature and then transmits the update to the target system. Olarig et al. does not teach that the BIOS receives a message from an authorized party. Further, Claim 1, at least, requires *a public key stored in non-volatile storage communicatively coupled to the BIOS*. Olarig et al. do not teach that the public key be stored in non-volatile storage communicatively coupled to the BIOS. Olarig et al. merely teach that the public key is stored. It could be stored in a temporary volatile location.

Olarig et al. teach only that an authenticated message is to be loaded as an upgrade, but is silent as to discarding the message, as required by Applicant's claims. Thus, this feature is not taught at the cited reference (Col. 4, lines 1-34). Olarig et al. do teach that if the upgrade causes the system to crash on reboot that the previous BIOS is loaded. However, this method is not the same as discarding an unauthenticated message, and results in inefficiencies from the required, failed, reboot.

The second digital signature of Olarig et al. is not relevant to the use of a GUID. The Examiner asserts that Mohammed et al. teach the GUID as recited in Applicant's claims. Applicant does not admit that Mohammed et al. is properly combined with Olarig et al. However, without conceding the validity of the combination, Mohammed et al. fail to teach *verifying that the system is an intended recipient of the message, wherein verifying comprises comparing an identifier in the message against a globally unique identifier (GUID) of the system, the GUID stored in the non-volatile storage communicatively coupled to the BIOS.*

Mohammed et al. teach an "application's GUID" at Col. 14, lines 42-60. The application's GUID is used to verify a download permit. Mohammed et al. teach a method where an application id identified as being authorized to run on a platform. In contrast, Applicant's claimed invention requires a GUID associated with the system, not an application. The GUID is used to verify that the system, or hardware platform, is authorized to receive a message authorizing an optional feature of the system resources. Mohammed et al.'s use of a GUID is not at all related to Applicant's claimed invention. Nor is there any suggestion in Mohammed et al. or Olarig et al. that a GUID may be used to uniquely identify a system for controlling optional features of a system resource in the system. Moreover, Olarig et al. do not teach controlling optional features of a system resource, but merely upgrading a BIOS in a system.

The Examiner has failed to provide *prima facie* evidence of obviousness, as Olarig et al. and Mohammed et al. fail to show every limitation of the recited claims, either individually or in combination. Thus, Claims 1, 3, 5, 6, 8, 10, 13, 16, 17, 19, 21, 22, 24-30 and 32 and their progeny are believed allowable.

Claims 4, 14 and 20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Olarig et al. and Mohammed et al. system as applied to Claims 3, 13 and 19 and further in view of USPN 5,230,052 to Dayan et al. (hereinafter, "Dayan et al."). This rejection is respectfully traversed based on the foregoing and following discussion.

As discussed above, Olarig et al. and Mohammed et al. fail to teach or suggest all of the elements of the base claims upon which Claims 4, 14 and 20 depend. Thus, Claims 4, 14 and 20 are allowable, at least, by being dependent from an allowable base claim.

With regards to combining these references with the teaching of Dayan et al., the Examiner asserts that Dayan et al. teach that the secure non-volatile location comprises a remote storage. In fact, Dayan et al. only teach that BIOS code is maintained in a remote memory. BIOS code is not the same as *writing the message into a secure non-volatile location*. Applicant's recited claim requires receiving a message from an authorized party and being able to authenticate the message with a digital signature and then verifying that the system GUID enables optional features of system resources, as specified in the message. At least at the cited reference (Col. 4, lines 3-13), Dayan et al. do not teach or suggest storing a received message in remote storage. Thus, the cited references fail to show each and every limitation of the claim.

The Examiner has failed to provide *prima facie* evidence of obviousness, as Olarig et al., Mohammed et al. and Dayan et al. fail to show every limitation of the recited claims, either individually or in combination. Thus, Claims 4, 14, 20 and their progeny are believed allowable.

Claims 7, 15 and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Olarig et al. and Mohammed et al. system as applied to Claims 1, 8 and 17 and further in view of U.S. Patent Application Publication No. 2001/0025312 to Obata (hereinafter, "Obata"). This rejection is respectfully traversed based on the foregoing and following discussion.

As discussed above, Olarig et al. and Mohammed et al. fail to teach or suggest all of the elements of the base claims upon which Claims 7, 15 and 23 depend. Thus, Claims 7, 15 and 23 are allowable, at least, by being dependent from an allowable base claim.

Claims 9 and 11 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Olarig et al. and Mohammed et al. system as applied to Claim 8 and further in view of USPN 6,182,219 to Feldbau et al. (hereinafter, "Feldbau et al."). This rejection is respectfully traversed based on the foregoing and following discussion.

As discussed above, Olarig et al. and Mohammed et al. fail to teach or suggest all of the elements of the base claims upon which Claims 9 and 11 depend. Thus, Claims 9 and 11 are allowable, at least, by being dependent from an allowable base claim.

Claim 31 is rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Olarig et al. and Mohammed et al. system as applied to Claim 27 and further in view of USPN

5,953,536 to Nowlin, Jr. (hereinafter, "Nowlin"). This rejection is respectfully traversed based on the foregoing and following discussion.

As discussed above, Olarig et al. and Mohammed et al. fail to teach or suggest all of the elements of the base claims upon which Claim 31 depends. Thus, Claim 31 is allowable, at least, by being dependent from an allowable base claim.

The Examiner asserts that Nowlin Jr. teaches *wherein the secure message comprises executable code to be used as a Dynamically Loaded Library (DLL), and wherein the DLL is to be stored in non-volatile storage coupled to the BIOS, and wherein the DLL is to be loaded by the BIOS at run-time*. In fact, Nowlin Jr. teaches only that a virtual device driver may be loaded into a DLL to enable the operating system (Windows®) to communicate with the APM BIOS. Nowlin Jr. does not teach that the DLL is a secure message comprising executable code to be loaded by the BIOS at runtime. Nowlin Jr. teaches away from this method at the cited reference (Col. 6, lines 44-54) by disclosing that the operating system "places into the default load configuration a virtual device driver." Applicant's claim requires that the message be received at the BIOS (see parent Claim 27) where the secure message is a DLL loaded by the BIOS at runtime.

The Examiner has failed to provide *prima facie* evidence of obviousness, as Olarig et al., Mohammed et al. and Nowlin Jr. fail to show every limitation of the recited claims, either individually or in combination. Thus, Claim 31 is believed allowable.

All of the pending claims are believed allowable.

CONCLUSION

In view of the foregoing, Claims 1, 3-11, 13-17 and 19-32 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-0221 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 6 June 2007

/ Joni D. Stutman-Horn /
Joni D. Stutman-Horn, Reg. No. 42,173
Patent Attorney
Intel Corporation
(703) 633-6845

Intel Corporation
c/o Intellevate, LLC
P.O. Box 52050
Minneapolis, MN 55402